EJPLT
ISSN 2704-8012

Cloud Computing Services: Towards a Digital Sustainability under EU Digital Law.

I servizi di cloud computing: verso la sostenibilità digitale nell'ambito della Strategia Digitale Europea.

FRANCO TRUBIANI
Researcher in Private Law, University of Naples 'Parthenope'

Abstract
The contribution aims to investigate, from the perspective of the private law scholar, the complex issue of cloud computing. The author dwells on the potential of this technology not only for the benefit of users and businesses, but also for the service of the public administration in the declared perspective of the search for a sustainable digital environment.
Next, the author analyses, in light of the recent European legal innovations, the main problems, with particular focus on the protection of personal data entrusted to the cloud, trying to hypothesise a new key to interpretation in order to propose new contractual models and reach a renewed responsibility of the cloud service providers.

Il contributo si propone di indagare, dalla prospettiva dello studioso di diritto privato, il complesso tema del cloud computing. L'autore si sofferma sulle potenzialità di questa tecnologia non solo a vantaggio di utenti e imprese, ma anche al servizio della pubblica amministrazione nella dichiarata prospettiva della ricerca di un ambiente digitale sostenibile.
In seguito l'autore analizza, alla luce delle recenti novità legislative europee, le principali problematiche, con particolare riferimento alla protezione dei dati personali affidati al cloud, cercando di ipotizzare una nuova chiave di lettura per proporre nuovi modelli contrattuali e giungere a una rinnovata responsabilità dei fornitori di servizi cloud.

Keywords: Digital Sustainability - Cloud services - Technological Innovation – Personal Data.

1. Cloud computing as a new technological tool to support digital sustainability.

Cloud computing services, or simply 'cloud', represent the latest model of access to computerized information systems through decentralized computer equipments.[1]

This refers to the on-demand reallocation of access to a shared processing system (such as networks, servers, storage, applications, and services) through which data and functions can be quickly shared.[2]

It is therefore a mode that allows all users to access large computing power without incurring significant economic efforts. This, therefore, requires providers to adapt to computer language, for example, to the standards determined by the owners of cloud distribution platforms.

Such services can be offered jointly by the same provider or, as usual, by different providers; in fact, the network of involved contractual relationships is indicated by the North American doctrine through the image of 'cloud provider contracts chains'.[3]

Often, cloud service providers do not only offer to the end users software applications or, more generally, content, such as music, video or books – or products sold by the same providers, but also make their platform available to

[1] The Cloud computing market in Italy has reached a value of 3.34 billion euros, an indicator of strong growth contributed to by the health emergency phase that has caused the adoption of cloud in SMEs to rise 42% from a previous year-on-year average of 30% (source: 2020 Report of the Observatory of Digital Transformation, Politecnico di Milano, available at https://www.osservatori.net/it/ricerche/osservatori-attivi/cloud-transformation). According to a Gartner consulting company report published on February 9, 2022, entitled 'Market Impact: Cloud Shift 2022 through 2025,' over the next three years, more than half of Italian corporate spending will shift to the cloud, and already in 2022, with this shift, more than 1.3 trillion dollars of IT corporate spending will be spent, which will grow to almost 1.8 trillion dollars in 2025; this is according to Gartner, compared to 41% in 2022, in three years, 51% of corporate spending, within markets dealing with application software, infrastructure software, business process services, and system infrastructure, will shift from traditional solutions to hybrid and multi-cloud systems.

[2] The National Institute of Standards and Technology (NIST), a division of the US Department of Commerce, established in its 2011 'NIST Definition of Cloud Computing' (available at http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf) that 'Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models'.

[3] WK Hon, C Millard and I Walden, 'Negotiating Cloud Contracts: Looking at Clouds from Both Sides Now' (2012) 16 *Stan. Tech. L. Rev.* 79, 121, point out that 'several entities may be involved in providing a single cloud service, including suppliers of hardware, software, and data center services. There may be chains of contracts between them. Contractual requirements may vary with the cloud 'stack' component under consideration'.

other providers to sell their services (for example in the gaming [4] or entertainment sector [5]), taking advantage of the 'Time to market' factor [6], typical of a net-strategy suitable for technological evolution, through a Lean type process rather than traditional[7], namely, a management style that aims to eliminate waste and to create excellent standardized processes at low cost with the contribution of people.[8]

A peculiar element that characterizes cloud models is the delivery of a service: it is specified, from now on, that this element reveals how the cloud is a model focused not on proprietary size, but precisely on the delivery of computer services by third-party providers, based on a paradigm already widely investigated by economic literature, which in this regard interpreted as a 'new culture of access'.[9]

The increasingly massive use of cloud technology for storing and/or processing data or a complex and integrated service of the indicated features, not only by private individuals but also by public administrations, in the form of the so-called 'community cloud' through which the service is made available to a specific community, represents today a fact that is fully acknowledged and that increasingly leads the interpreter to think about the possible solution of new problems arising from the use of a technical infrastructure whose modes of operation were mostly ignored by the user until few years ago (consumer and non-consumer) and whose activities were subtracted from any regulation.[10]

The European Union itself seems to indicate the study of the legal problems related to the use of cloud computing services in the 'New Consumer Agenda - Strengthening consumer resilience for sustainable recovery' in which the

---

[4] Recently, the article M Longan and others, 'Cloud gaming demystified: an introduction to the legal implications of cloud-based video games' (October 27th, 2021), *Queen Mary Law Research Paper*, No. 369/2021, discusses the specific sector of cloud gaming. They propose the existence of a cloud model called Gaming as a Service (GaaS), as a subtype of the Infrastructure as a Service (IaaS) model.

[5] It appears to be clear that having access to cloud distribution platforms represents a key tool for helping to spread and share original works. For more information on this topic, see V Falce, 'Standard e cloud computing' (2015), 29(2) *Dir. ind.*, 155 ff.; ML Montagnani, *Il diritto d'autore nell'era digitale* (Giuffrè 2012) 115 ff.; A Musso, 'La proprietà intellettuale nel futuro della responsabilità sulla rete: un regime speciale?' (2010), 26(6), *Dir. inf.*, 795 ff.; AM Gambino, '*Cloud, diritto d'autore e nuovi modelli di circolazione giuridica*', in *Studi per Luigi Carlo Ubertazzi. Proprietà intellettuale e concorrenza* (Giuffrè 2019), 347 ff.; A Bertoni and ML Montagnani, 'La modernizzazione del diritto d'autore e il ruolo degli intermediari internet quali propulsori delle attività creative in rete' (2015), 31(1) *Dir. inf.*, 111.

[6] ME Mcgrath, *Product strategy for High Technology Companies* (McGraw Hill 2001) 55-58.

[7] The references offered by the studies of merchandising sciences seem very useful to understand the utility of the cloud as a tool for companies (and, in particular, for micro-enterprises) in order to accelerate the sales processes and get to the market faster. The compression of response times to the market also makes the company competitive from a strictly economic-financial point of view, since the company could more quickly reach the break-even point, that is, the moment when costs and revenues are balanced and new products begin to generate profit with stable or decreasing investments compared to the launch phase.

[8] But not only that: think about the perspective of the so-called 'cloud robotics', outside the scope of this study, where there is a shift of part of the intelligence of the robot to the cloud through the sharing of information and the abstraction of the hardware used. In the current cloud robotics scenario, the robot is offered almost unlimited computational power in the cloud compared to its real needs. An obvious advantage over the capacity that can be offered by the processing and storage resources on board the machine and, as a result, important functionalities can be performed with a level of accuracy and execution speed that is significantly higher.

[9] The reference obviously goes to J Rifkin, *The age of access* (Penguin 2000).

[10] L Ammannati, '*Il paradigma del consumatore nell'era digitale. Consumatore digitale o digitalizzazione del consumatore?*', in F Capriglione (eds), *Liber Amicorum Guido Alpa* (Cedam 2019), 436.

Commission indicated among the new priorities and crucial points of action for the so-called consumer welfare to be worked on until 2025: specifically, point 3.2. of the Agenda, called 'Digital Transformation' aims, in the declared perspective of a development in line with the principles of sustainability and green development, to facilitate the effective right of people to the portability of their data (as widely recognized in the new proposed Data Act Regulation), in the perspective of creating a true single market and European common data spaces.

In this sense, therefore, there is an European trend towards the search for a so-called 'sustainability of the digital environment', that is, the need to build a digital system capable of capturing the potential of technological evolution and, at the same time, of protecting the fundamental rights of individuals.

In the current highly innovative and complex digital context, this investigation aims to analyze, from a strictly civil law point of view, the topic of cloud computing services, focusing in particular on contractual aspects, analyzing the impact that the classification of these services has on our civil code and those related to the responsibility of the cloud service provider, identifying the multiple legal profiles that the use of cloud services entails compared to traditional legal categories in the context of digital sustainability.

2. The 'Cloud First' principle in the Italian National Recovery and Resilience Plan (PNRR).

The Three-Year Plan for Information Technology in Public Administration 2017-2019 approved by the Prime Minister's Decree of 31 May 2017 launched a process of rationalisation and upgrading of the Information and Communication Technology infrastructures of the public administration, based on the technological principle of 'cloud first'.

The aim is to enable administrations to make more efficient and flexible use of Information and Communication Technology resources, with high levels of cost-effectiveness, reliability and security: this is also with a view to fostering the full interoperability of data and an offer of services that is increasingly tailored to the needs of citizens and businesses.[11]

The many legislative interventions aimed at the digital transformation of the Public administrations (P.A.) have created an evolution strategy based on several principles, among which is the so-called 'cloud first'.

According to this principle, P.A. when defining a new project or developing new services one must prioritise the adoption of the cloud paradigm over any other technology.

The qualification process that cloud service providers must undergo involves three main steps: applying for, obtaining and maintaining qualification.

In line with the requirements of the Three-Year Plan, the Digital Italy Agency conducted a census of the Information and Communication Technology assets

[11] G Napolitano, 'Il partenariato pubblico-privato per la realizzazione del Polo strategico nazionale' (2021), 27(6), *Giornale dir. amm.*, 704.

of public administrations, aimed at classifying the relevant infrastructures in terms of reliability and security.[12]

The census, whose results were published as an annex to Agency Resolution No. 1 of 14 June 2019, revealed a picture of high fragmentation, inadequate security levels and high inefficiency in terms of expenditure. Many data center were found to be energy inefficient, obsolete, insecure and wasteful.

In the light of these data, Decree Law No. 76 of 16 July 2020 on 'Urgent measures for digital simplification and innovation' converted into Law n. 120 of 11 September 2020, in order to promote 'the development of a highly reliable infrastructure located throughout the national territory for the rationalization and consolidation of information processing center', provided that central administrations with type B data center, in compliance with the principles of efficiency, effectiveness and cost-effectiveness of administrative action, are obliged to migrate their information processing center and related IT systems to suitable facilities. The latter, therefore, should be identified among: (a) the National Strategic Pole to be set up, (b) infrastructures that already exist and meet the requirements, (c) Sogei's infrastructure, if made compatible with the requirements set forth in the specific regulation of the Cybersecurity Agency or (d) public cloud solutions for non-critical services.

The same Decree-Law No. 76/2020, as further amended by Decree-Law No. 82 of 14 June 2021, converted into Law No. 109 of 4 August 2021, also established that the Cybersecurity Agency, through its own regulation, shall identify the minimum levels of security, processing capacity, energy saving and reliability of digital infrastructures for public administration and define the quality, security, performance and scalability, interoperability and portability characteristics of cloud services for public administration.

The same regulation should further identify the terms and modalities by which the administrations must carry out the aforementioned migrations to technologically suitable structures.

In particular, according to the 'Italian Cloud Strategy' although international practices and technical standards are widely applied by cloud service providers, given the criticality of the data and services involved, the cloud migration strategy cannot disregard a qualification process of public cloud providers and their services. Moreover, qualification should not be limited to assessing the security aspects mentioned above, but also architectural and organisational ones, as these too can affect the resilience of the services provided, e.g. in vendor lock-in situations.

Another important direction, in line with the recent initiatives and directives of the European Digital Agenda, is that of the standardisation, harmonisation and interoperability of cloud services: in this perspective, with the involvement

[12] R Carleo, 'Il futuro della memoria digitale' (2022), 1(1), *La Magistratura*, 1 ff., gives a lucid reflection on the issue of digital data storage, analysing, in particular, the possible problems linked to the new frontier of 'neuromorphic computing' (which should enable machines to learn and think). He concludes his paper by arguing that 'who knows, then, if machines themselves might not become capable of choosing and selecting the data that must be properly stored in time and remembered in digital memory. Hoping for an optimistic view of the developments of artificial intelligence, it is precisely the machines - if they are well programmed to guarantee the purpose of maintaining democratic control over data and also the most appropriate choices on data storage - that could save us from their dictatorship'.

also of Italy, the GAIA-X project was launched at the end of 2019 with the aim of developing common requirements for a European data infrastructure.

The implementation of the National Strategic Pole was therefore included among the qualifying projects of the National Recovery and Resilience Plan transmitted by the Italian Government to the European Commission on 5 May 2021 and, on the latter's proposal, definitively approved by the European Council with the execution decision of 13 July 2021.

Within the measure 'Digitalization, Innovation and Security in the Public Administration' of the NRP, investment 1.1 (Digital Infrastructure) in the amount of EUR 900 million and investment 1.2 (Enabling and Facilitating Migration to the Cloud) in the amount of EUR 1,000 million are planned.

The National Recovery and Resilience Plan (so-called PNRR), therefore, considers cloud computing an essential tool to promote the improvement of IT infrastructures and services of the public administration. The Italian government's declared need is to achieve a proximity cloud in the next few years for at least a couple of reasons: a) there is undoubtedly a technological need (consider for instance of the Internet of Things or Driverless cars) for which it would be more useful for cloud servers to be geographically close to the places of production of the various technological phenomena; b) proximity goes towards realising true digital sustainability in which data are always close to where they are produced, in full respect of the ecological transition & digital sustainability.[13]

3. Cloud Services and EU Law Agenda.

In Europe the first regulatory indications on the cloud date back a few years: in its Communication dated 19th April 2016 on the European Cloud Initiative, the EU Commission pointed out two pillars.

The first pillar is the development of an adequate European infrastructure (European Data Infrastructure), consisting of networks for ultra-fast connectivity and adequate HPC (High Performance Computing) resources.

The second pillar is the provision of European research for a high-quality Cloud system that focuses on the principle of data sharing (European Open Science Cloud – EOSC). If, for the European Data Infrastructure, the issues to be addressed are typical of the infrastructure policy, including the use of European funds and the modalities of private public cooperation, the second pillar deserves a brief analysis – as the process to realize the EOSC is central to the problem of the relationship between new services and protection of rights. The main objective of the EU Commission through the EOSC is to overcome the current fragmentation of databases and the inadequate integer capacity, and facilitate the sharing and reuse of information.

In the current context of the EU Digital Law Strategy there are some provisions that are relevant for Cloud Service Providers. Reference is made in particular to: (a) the General Data Protection Regulation (GDPR), already adopted and in force from 25th May 2018 (which will be discussed specifically

[13] S Epifani, *Sostenibilità digitale. Perché la sostenibilità non può fare a meno della trasformazione digitale* (Digital Transformation Institute 2020).

in the next paragraph); (b) the proposed Regulation on European 'Data Act'[14]; (c) the EU Cybersecurity Strategy (in particular the proposal for a Directive on measures for a high common level of cybersecurity across the EU - NIS2 Directive – Directive 2022/2555/UE on measures for a high common level of cybersecurity across the Union); and (d) some rules on the liability of providers of Internet services (Regulation of the European Parliament and of the Council 2022/2065/EU on a Single Market For Digital Services and amending Directive 2000/31/EC - Digital Services Act) will be included.

With regard to the critical issues related to cloud services, the Proposal 'Data Act' provides for a strengthened right to portability of cloud computing services, facilitating consumers in switching from one cloud data processing service provider to another, preventing vendor lock-in.

On this point, it is envisaged to phase out pass-through tariffs in the three years following the coming into force of the data regulation and, in the medium term, the possibility of introducing a control mechanism on them (Art. 25 Data Act).

The Commission aims to provide a new interoperability framework for the development of common European data spaces; and it does so by empowering European standardization organizations to draft harmonized interoperability standards. This is done with the objective of going beyond the initial EU General Data Protection Regulation (GDPR) approach to personal data portability by extending the remit of this right to non-personal data. This was previously hindered by the lack of important technical specifications – such as for APIs – and by legal language that foresaw interoperability 'only where technically feasible'. Two types of actors are the main targets of such technical requirements: 'operators of data spaces' and 'cloud computing providers'. They will be obliged to enable users' data portability and switchability across digital services.

Finally, Chapter VII touches on the cross-border transfer of non-personal data. The measure, in article 27, compels cloud computing providers to take all reasonable technical, legal and organizational measures, including contractual arrangements to 'prevent international transfer or governmental access to non-personal data held in the Union where such a transfer or access would create a conflict with Union law (…)'.

This means that the Commission will be in charge of developing guidelines consistent with the recommendations of the European Data Innovation Board, to be established under the Data Governance Act (DGA)[15].

At a practical level, the proposed rules for international data transfers have important implications for cloud computing service providers as the Commission is strongly restricting foreign governments' access to non-personal data stored in Europe, unless these are based on international agreements, such as mutual legal assistance treaties.

This seems to be a direct response to the previous controversies sparked by the CLOUD Act, which foresees executive agreements between the US

[14] Please note that the approval by the EU Council's on 27th of November 2023 is subsequent to the date the author sent the article to the Journal's editorial office.

[15] On Data Governance Act see S Tranquilli, 'Il nuovo citoyen européen nell'epoca del Data governance act' (2022), 1-2, *Digital Politics*, 179 ss.

Government and third countries' law enforcement agencies to grant reciprocal access to data held by cloud providers in each other's territories. In the absence of international agreements, the DA allows for transfer of data hosted by cloud computing providers if and only if the third country provides an equitable level of protection to EU law.

If these are met, the minimum amount of data permissible in response to a request shall be transmitted. This is in line with the data transfer regimes stipulated in the GDPR for personal data and the DGA for non-personal data.

The European Commission replaced the NIS Directive, the first piece of EU-wide legislation on cyber security, with the NIS 2 Directive in order to respond to the growing threats posed by digitalisation and the wave of cyber attacks and at the same time strengthen security in companies and supply chains, simplify reporting obligations and introduce stricter supervisory measures and enforcement requirements, including harmonised sanctions throughout the EU.

Compared to the original NIS Directive, NIS2 may expand the number of regulated organizations by 10 times or more. This expansion may lead to new compliance challenges for organizations of all sizes and place additional strain on national cybersecurity authorities tasked with oversight and enforcement.

Companies identified by the Member States as operators of essential services in the above-mentioned areas will have to take appropriate security measures and inform the competent national authorities of serious incidents, e.g. data leaks. Major providers of digital services, such as search engines, cloud computing services and online marketplaces, will have to comply with the security and notification requirements of the directive.

For example, Art. 23 NIS2 establishes a framework for notifying eligible national authorities and relevant customers of any cyber incident with a significant impact in terms of operational disruption, financial loss, or physical harm. In the event of a significant incident, covered organizations will be required to file an initial report within 24 hours, a requirement that will test their reporting capabilities. Organizations will then be required to file a more detailed report within 72 hours, and a final, comprehensive report within one month.

The Digital Services Act (DSA) included Cloud Service Providers among the recipients of due diligence obligations.

In 'Considerando' n. (13) and n. (28) of the DSA, cloud computing is expressly referred to as an intermediary service included in the Framework. Depending on the concrete operation of the cloud computing service, the rules on exemptions from liability for Cloud Service Providers are the same as for providers of mere conduit, caching or hosting services, which in turn are almost identical to those laid down in Directive 2000/31/EC. Apparently, the only real change that the DSA introduces for the world of cloud computing would be in having made it uncontroversial that a Cloud Service Provider is exempt from liability for what the recipients of the services (its customers) do under the same conditions and with the same exceptions that already applied and will continue to apply, as the case may be, to providers of mere conduit, caching, or information storage services.

Regarding the Internet Service Provide (ISP) liability regime, cloud services must be equated with online platforms[16].

The ISP's liability is excluded if the ISP is not actually aware that the customer's or user's activity (or information) is unlawful and, as far as actions for damages are concerned, is not aware of facts or circumstances that make the unlawfulness of the activity or information apparent (non-knowledge) and if - as soon as it becomes aware of such facts - the ISP acts immediately to remove the information or to disable access to it (timely removal).[17]

In concrete terms, in order to benefit from the limitation of liability, a Cloud Service Providers will have to act immediately to remove the information or to disable access to it as soon as it is informed or becomes aware of the unlawful activities. In addition, it shall take appropriate organisational and technical measures upon being informed, or becoming aware if it has evidence of unlawful activities.

Article 16 of the DSA requires ISPs (including, therefore, Cloud Service Providers) to create mechanisms that enable users to notify the presence of illegal content on their service, and to provide sufficiently precise and adequately reasoned explanations as to why they consider it to be illegal, a clear indication of where it is located, their identification data, and confirmation of their good faith belief in the accuracy and completeness of the information and statements made.

In addition, all ISP's must notify the person or entity issuing the alert of their decision on the information to which the alert relates, providing information on the possibilities for appeal.

Finally, under Article 18 of the DSA, insofar as it qualifies as a hosting provider, even a Cloud Service Provider, if it becomes aware of information that leads to the suspicion that an offence has been committed, is being committed, or is likely to be committed involving a threat to the life or safety of one or more persons, must inform the judicial or law enforcement authorities without delay, providing the available information. Adding together the burden of coping with the reporting and action mechanism governed by Article 16 and the notification of suspected offences under Article 18, it seems clear that the only way for an ISP to be compliant is to equip itself with appropriate procedures, defining roles and responsibilities.

4. The protection of personal data entrusted to the cloud.

A profile of particular relevance to cloud computing concerns the protection of the confidentiality of personal data. The model in question involves the transfer of data, very often generating a cross-border circulation of the same.

[16] The DSA applies to a wide range of intermediary service providers that are classified according to (i) the type of information society service provided and according to (ii) their respective sector and/or size, with special reference to digital platforms.

[17] R Bocchini, '*La responsabilità extracontrattuale del provider*', in R. Bocchini (eds), *Manuale di diritto privato dell'informatica* (Esi 2023), 533 ff.

As it has been correctly pointed out[18], in fact, the distribution model of IT services has been facilitated by the speed of network connections and the ability to aggregate a previously unimaginable amount of computing power in huge data center.

Cloud service providers have data farms located in various parts of the world, managed according to efficiency criteria implying the mobility of the data stored in the 'cloud': these data, in fact, do not reside permanently in the same server, but are continually moved from one server to another due to their optimal allocation, in order to achieve a better management of IT resources.

This process, however, can lead to a breach of confidentiality not only of the personal data of users but also of entire databases of e.g. telephone operators or credit institutions.[19] In the event that a customer makes use of data storage services on the cloud, the risks of an attack or unauthorised access by third parties would multiply, especially in the event that the data transfer is implemented outside European borders.

The need to protect personal data requires the identification of a data controller who is liable for any violations of the General Data Protection Regulation that must receive protection regardless of the territory of the states (art. 3 GDPR).

The problem of the effective application of the protection thus shifts from the difficulty of imposing the legislative rule to that of identifying the data controller, which may not always be easy and immediate to identify.

In fact, in practice, there seems to be a certain distance between the data controller under Art. 4(7) GDPR (usually the client company that relies on a cloud service provider) and the data processor under Art. 4(8) (the cloud service provider): this is because, given that the sector in question is often characterised by the outsourcing of services, which means, in essence, that the longer the cloud 'chain' goes on, the more difficult it becomes for the data controller to ensure compliance with the GDPR.

The growing adoption of networked and distributed architectures, which provide for the compartmentalisation and division of functions relating to data processing, with integrated and competing competences, sees, in fact, the presence of a plurality of data controllers and an integration of their respective competences, often relegating the data controller's function to a more formal than substantial role. The latter, in complex organisations, has the task of defining the purposes of processing and is responsible in the event of unlawful processing, but often lacks effective power of determination and control over the processing methods delegated to third parties.[20]

The flow of data resulting from the provision of cloud computing services can be qualified as a flow between two autonomous data controllers or between a data controller and a data processor. In the first case, the autonomy of the parties' processing would exclude the client's liability for any wrongdoing on the part of the cloud service provider; when, on the other hand,

---

[18] A Mantelero, '*La privacy all'epoca dei big data*' in V Cuffaro, R D'Orazio and V Ricciuto (eds), *I dati personali nel diritto europeo* (Giappichelli 2019), 1216, nt. 2.

[19] TE Frosini, 'Il costituzionalismo nella società tecnologica' (2021), 36(39, *Dir. inf.*, 474.

[20] A Mantelero, 'GDPR tra novità e discontinuità – Gli autori del trattamento dati: titolare e responsabilità' (2019), 171(12), *Giur. it.*, 2778.

the cloud service provider is considered an autonomous data controller, the client would no longer have any management function in relation to the data processing carried out through the cloud service.

There has been much debate on the legal qualification of the provider, i.e. on whether this contractual figure can be attributed to the role of data controller or data processor.

By virtue of the nature of the professional activity exercised by the cloud service provider, the majority thesis tended to attribute to him the status of processor, i.e. of legal entity entrusted by the customer with the storage of data, as if he were a sort of agent precisely because of the nature of the activity exercised by the cloud service provider.

On the contrary, in B2B relations, the cloud user has the status of controller, i.e. of data controller.

However, on closer inspection, the qualification of the cloud service provider as processor cannot be recognised a priori: this would seem to depend on the margin of bargaining power granted to the cloud user when drawing up the contractual regulation.

In fact, it is possible to resort to the figure of the so-called co-processors provided for in Article 26 GDPR.

Co-processing is established whenever two or more data controllers jointly determine the purposes and means of processing: this is particularly appropriate for the management of cloud computing services where there may be a risk of confusion between the various roles.[21]

The GDPR has intervened to a very marked extent in the definition of the obligations placed on the provider, setting out in Articles 28, 32 and 34 a series of expedients and technical and organisational security measures[22] that each processor is required to adopt so that the data processing offered in the provision of the service can meet the requirements dictated by the same Regulation in order to ensure maximum protection of the rights of the persons concerned by the processing.

The issue of personal data protection becomes even more complex when the data controller, as a professional-businessman, uses cloud services to store personal data of third parties. Indeed, companies and professionals are increasingly relying on cloud technology to manage aspects of their business, outsourcing the storage of documents containing data, including sensitive data, both of their business partners and/or subordinate collaborators, and of their customers.

In this context, therefore, it is the professional client who, in choosing a given service among those available on the web, autonomously defines the

[21] L Valle and Others, '*Struttura dei contratti e trattamento dei dati personali nei servizi di cloud computing alla luce del nuovo Reg. 2016/679 UE*' (2018), 18(1), *Contr. impr. Eur.*, 399.

[22] The security measures imposed by the GDPR include: pseudonymisation, encryption of personal data, the ability to ensure the confidentiality, integrity, availability and resilience of systems and services on a permanent basis, and the ability to restore data availability and access in the event of physical or technical disruptions. On this point, the Article 29 Data Protection Working Party of Directive 95/46/EC already expressed its opinion in 2010 (Opinion No. 3 of 2010) that it was necessary to adopt a process aimed at the adoption of legal, organisational and technical measures for the protection of personal data, including through the development of specific organisational models, also aimed at demonstrating that the data processing operations already carried out were carried out in compliance with the European Privacy Regulation then in force.

management modalities and the security regime to which to subject the information in his possession . And if this is the case, then the owner must take care to obtain the consent of the person directly concerned by the processing, even before entrusting such data to the processor or, moreover, to possible subprocessors.

This notwithstanding, if at a theoretical level it is easy to deduce that the burden falls on the controller, in practice it may be difficult for the latter to prepare complete information documents to be submitted to the person directly concerned by the processing, in the absence of the support and cooperation of the cloud service provider.

It should also be noted that, although the possibility of establishing such networks of subprocessors in B2B relations has been recognised, the GDPR, which is designed to protect the personal data of natural persons, mainly places the responsibility on the data controller or, in the cloud context, on the professional client.

The rule can be deduced from a reading of Article 28(1) GDPR, which places an obligation on the data controller to choose only 'data controllers providing sufficient guarantees to implement appropriate technical and organisational measures so that processing meets the requirements of this Regulation and ensures the protection of the rights of the data subject', on pain of liability and/or co-liability.[23]

It has been held that the binding nature of the agreement pursuant to Article 28(3) GDPR has a twofold effect on the controller[24]: on the one hand, the controller cannot unilaterally withdraw from the appointment without terminating the main agreement and, on the other hand, the latter cannot legitimately refuse to enter into an act of appointment necessary under the main contractual relationship.

This does not prevent the appointment as controller from having binding effects also vis-à-vis the controller, given that Article 28(3) itself admits the possibility of obligations on the controller.

As regards, instead, the sanctioning profile, Article 82 GDPR has established two forms of liability: one for the controller, as the data controller, who is liable for the damage caused by its processing in breach of the GDPR; the other for the processor, i.e. the data controller, who is liable for the damage caused by the breach of confidentiality in the event of failure to comply with the

[23] On this point, see the decision of the Swedish Data Protection Authority (11 December 2020) - available at https://edpb.europa.eu/news/national-news/2020/university-failed-sufficiently-protect-sensitive-personal-data_it - which fined Umeå University 550,000 Swedish kronor for violating data protection regulations. Specifically, however, no sanction was imposed under the GDPR as the events had occurred before its entry into force. Umeå University, among other violations, allegedly processed special categories of personal data concerning the sexual life and health of its employees by storing them in a cloud storage service of a well-known American company, without designating an appropriate controller. The Swedish Data Protection Supervisor's decision appears relevant as it follows in the footsteps of the well-known 'Schrems II' ruling, arguing that the transfer of personal data contained in cloud storage to the United States would in itself trigger a high risk to personal data as data subjects would be restricted in their ability to assert their rights.

[24] L Bolognini - E Pelino, '*Art. 28. Responsabile del trattamento*', in edited by L Bolognini and E Pelino (eds), *Codice della disciplina privacy* (Giuffrè 2019), 222.

obligations laid down by the GDPR or when it has acted in a manner inconsistent with or contrary to the lawful instructions of the data controller.[25]

In the latter hypothesis, in B2B cloud relationships, the processor is obliged to compensate for damages, including non-pecuniary damages, suffered by the data subject, in addition to being liable for any administrative sanctions imposed by the competent supervisory authorities.

5. Perspective and conclusions.

The impression one gets from these initial introductory remarks on cloud legal issues, observed through the prism of the private law scholar, is that of a topic that appears worthy of further exploration and analysis, given also the speed of technological and legislative evolution.

As correctly acknowledged by an important voice in the current philosophical debate, the advent of the digital 'is changing the conception we have of ourselves'[26] and is going to modify the habits of life of the human being, entailing decisive implications also of a legal nature.

Perhaps, then, the risk that seems to be running is that of preserving an anachronistic law in the face of technological evolution. More specifically, private law itself, through a decisive interaction between the discipline of contracts, the protection of personal data and digital identity, as well as intellectual property, is increasingly being called upon to confront increasingly complex and difficult challenges that continue to call into question its traditional balances.

We can, however, try to make some reflections on the state of the art and possible future prospects.

In addition to the decisive role of European regulation, it seems worth mentioning the importance of the contract for better regulation of cloud computing.[27]

An analysis of commercial practice also reveals the absence of any type of guarantee, the exclusion of liability for damages caused to the user, and the presence of clauses limiting the extent of identifiability for damages caused by the cloud service provider, circumstances that pose delicate problems as to the admissibility of such clauses in our legal system.

The clauses related to the exclusion of liability and limits on identifiability, moreover, are accompanied by the indication that the cloud computing service is normally provided 'as is', in other words 'as available'. The definition of the regulatory regime, in fact, represents a fundamentally important step: the cloud service provider is often located beyond national borders, and user data

---

[25] N Busca, '*Cloud computing e tutela della privacy nei rapporti commerciali B2B*' (2020), 26(11), *Studium juris*, 1336.

[26] L Floridi, *Il verde e il blu. Idee ingenue per migliorare la politica* (Raffaello Cortina Editore 2020) 77, according to which 'the 'onlife' mode is increasingly underpinning our daily activities. It defines the way we communicate and interact, learn, work, shop, take care of our health, have fun, cultivate our relationships; the way we interact with the legal, financial, political world; even the way we wage war and maintain or promote peace...the digital has changed the way we view ourselves, our world, and our temporality'.

[27] On this point see F Trubiani, '*I contratti di cloud computing: natura, contenuti e qualificazione giuridica*' (2022), 38(2), *Dir. inf.* 395 ff.

are sent, via the network, to systems located in countries whose legal systems provide for a privacy protection regime that is inferior to the European one.

It is therefore necessary to seek to construct a balanced negotiating settlement that allows the customer to have greater certainty.

Since the solutions offered in the area of cloud computing are represented by a wide variety of possible architectures, service models, combination of technologies made available and software adopted, it will be necessary to make explicit in the contract all the assumptions underlying the choice of the solution adopted and the service provider.

Service reliability, authentication and authorisation, cryptography, security incident management and reporting, logging and monitoring, security auditing and verification, vulnerability management and governance of security controls are the main points to be included in an acceptable level of security: the definition of shared technical standards represents the first step in order to accomplish a system of legal rules inspired by and, in a certain sense, able to drive technological development.

An alternative or at least competing scenario, then, could be that of envisaging a form of co-regulation[28], in which the rules are suggested by the market (perhaps through the contribution of the sector's stakeholders, such as the Cloud Security Alliance and of the scholars of new technologies law) and shared by the sector's authorities, following the 'regulatory circle' scheme.[29]

That is, it is a bottom-up mechanism that starts from the market's regulatory drive and introduces rules into the system - or at least immediately operational guidelines - that can then, if necessary, be taken into consideration by the legislator and translated into regulatory precepts.[30]

In the American literature, the development of 'best practices' guidelines is seen as a positive way to effectively regulate these contractual relationships, in particular to facilitate data portability in the cloud[31]: on closer inspection, codes of conduct may also be useful, more generally, to better define the cloud service provider's policy on the retention of users' personal data.

At the end of these considerations, however, the impression is that we are still faced - on the one hand - with a fragmented and still undefined regulatory framework and - on the other - with the need to proceed with the construction of appropriate contractual models for the cloud sector: in this sense, therefore, the role of the interpreter seems important, who will necessarily have to go into the individual issues that have only been hinted at here in greater depth.

---

[28] The term 'co-regulation' is ambiguous by nature. The expression is often used as a generic term to refer to forms of cooperation between market and authorities that are instrumental in the pursuit of regulatory objectives. Co-regulation is generally understood as a form of stakeholder regulation that is promoted, steered, guided or controlled by a third party (be it an official body or an independent regulator) usually endowed with powers of scrutiny, control and, in some cases, sanctioning. On the co-regulation problem see U Malvagna - M Rabitti, 'Filiere produttive e Covid-19: tra rinegoziazione e co-regolazione' (2020) 4(3), *Nuovo dir. civ.*, 369 f.

[29] F Bassan, *Potere dell'algoritmo e resistenza dei mercati in Italia* (Rubbettino 2019).

[30] On the other hand, as recently pointed out by A. Zoppini, *Il diritto privato e i suoi confini* (Il Mulino 2020) 28 f., there are rules and principles (such as those shared in international trade) that impose themselves in private relationships by their own force and that, insofar as they are recognised and shared, perform a normative function independently of their formal adoption.

[31] K Żok, 'Cloud Computing Contracts as Contracts For The Supply Of Digital Content: Classification and Information Duty' (2019), 13(2), *Masaryk University Journal of Law and Technology*, 151.